



PCT/BR03/101

REC'D 20 AUG 2003

WIPO

PCT

REPÚBLICA FEDERATIVA DO BRASIL
Ministério do Desenvolvimento, da Indústria e Comércio Exterior.
Instituto Nacional da Propriedade Industrial
Diretoria de Patentes


CÓPIA OFICIAL

PARA EFEITO DE REIVINDICAÇÃO DE PRIORIDADE

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

O documento anexo é a cópia fiel de um
Pedido de Patente de Invenção
Regularmente depositado no Instituto
Nacional da Propriedade Industrial, sob
Número PI 0202843-3 de 23/07/2002.

Rio de Janeiro, 29 de julho de 2003.


GLÓRIA REGINA COSTA
Chefe do NUCAD
Mat. 00449119



Protocolo

23 JUL 16 52 28 007310

Número (21)

DEPÓSITOPedido de Patente ou de
Certificado de Adição

PI0202843-3

depósito

Número e data de depósito

Ao Instituto Nacional da Propriedade Industrial:

O requerente solicita a concessão de uma patente na natureza e nas condições abaixo indicadas:

1. Depositante (71):

1.1 Nome: TAUÁ BIOMÁTICA LTDA

1.2 Qualificação: SOCIEDADE BRASILEIRA

1.3 CNPJ/CPF 04.983.825/0001-24

1.4 Endereço completo: AV. PRESIDENTE VARGAS 417, 5º ANDAR PARTE CENTRO RIO DE JANEIRO 20071-000 BR

1.5 Telefone:
FAX:☐ continua em folha anexa

2. Natureza:

☒ 2.1 Invenção☐ 2.1.1 Certificado de Adição☐ 2.2 Modelo de Utilidade

Escreva, obrigatoriamente e por extenso, a Natureza desejada: INVENÇÃO

3. Título da Invenção, do Modelo de Utilidade ou do Certificado de Adição (54):

EQUIPAMENTO CHANCELADOR DIGITAL PARA A ASSINATURA DE DOCUMENTOS ELETRÔNICOS,
INTERFACE DE PROGRAMAÇÃO DE APLICAÇÃO SEGURA PARA ACESSO A UM EQUIPAMENTO
CHANCELADOR DIGITAL, MÉTODOS ELETRÔNICOS PARA CADASTRAMENTO DE IMPRESSÃO☒ continua em folha anexa

4. Pedido de Divisão do pedido nº.

5. Prioridade Interna - O depositante reivindica a seguinte prioridade:

Nº de depósito

Data de Depósito / /

(66)

6. Prioridade - O depositante reivindica a(s) seguinte(s) prioridade(s):

| Pais ou organização de origem | Número do depósito | Data do depósito |
|-------------------------------|--------------------|------------------|
| | | / / |
| | | / / |
| | | / / |

☐ continua em folha anexa

DIGITAL UTILIZANDO UM EQUIPAMENTO CHANCELADOR DIGITAL E PARA ASSINAR DIGITALMENTE
DOCUMENTOS A PARTIR DA IDENTIFICAÇÃO POSITIVA DE UM USUÁRIO

02
27

Inventor (72):

() Assinale aqui se o(s) mesmo(s) requer(em) a não divulgação de seu(s) nome(s)
(art. 6º § 4º da LPI e item 1.1 do Ato Normativo nº 127/97)

7.1 Nome: EDUARDO ROSEMBERG DE MOURA

7.2 Qualificação: BRASILEIRO, ANALISTA DE SISTEMAS

7.3 Endereço: RUA BULHÕES DE CARVALHO 378 APT0. 301 COPACABANA RIO DE JANEIRO RJ BR

7.4 CEP:

7.5 Telefone

☒ continua em folha anexa

8. Declaração na forma do item 3.2 do Ato Normativo nº 127/97:

☐ em anexo

9. Declaração de divulgação anterior não prejudicial (Período de graça):
(art. 12 da LPI e item 2 do ato Normativo nº 127/97:

☐ em anexo

10. Procurador (74):

10.1 Nome e CPF/CGC MONTAURY PIMENTA, MACHADO & LIOCE S/C LTDA.

29.416.450/0001-41

10.2 Endereço AVENIDA ALMIRANTE BARROSO 139 GRUPO 703 CENTRO RIO DE JANEIRO RJ

10.3 CEP: 20031-005

10.4 Telefone 2524-0510

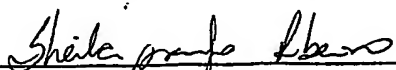
11. Documentos anexados (assinale e indique também o número de folhas):
(Deverá ser indicado o nº total de somente uma das vias de cada documento)

| | | | | | |
|-------------------------------------|-----------------------------------|----------------------------|-------------------------------------|---------------------------|---------|
| <input checked="" type="checkbox"/> | 11.1 Guia de recolhimento | 1 fls. | <input checked="" type="checkbox"/> | 11.5 Relatório descritivo | 21 fls. |
| <input checked="" type="checkbox"/> | 11.2 Procuração | 1 fls. | <input checked="" type="checkbox"/> | 11.6 Reivindicações | 2 fls. |
| | 11.3 Documentos de prioridade | 0 fls. | <input checked="" type="checkbox"/> | 11.7 Desenhos | 8 fls. |
| | 11.4 Doc. de contrato de trabalho | 0 fls. | <input checked="" type="checkbox"/> | 11.8 Resumo | 1 fls. |
| <input checked="" type="checkbox"/> | 11.9 Outros (especificar): | DOC. DE CESSAO DE INVENTOR | | | 1 fls. |
| | 11.10 Total de folhas anexadas: | | | | 35 fls. |

12. Declaro, sob penas da Lei, que todas as informações acima prestadas são completas e verdadeiras

RIO DE JANEIRO, 23/07/2002

Local e Data


Assinatura e Carimbo
MONTAURY PIMENTA, MACHADO & LIOCE S/C LTDA.
CGC-MF 29.416.450/0001-41

Nome: MARCIO CAMPOS DE LIMA

Qualificação: ANALISTA DE SISTEMAS:

Endereço: RUA COELHO NETO 52 APT. 804 LARANJEIRAS RIO DE JANEIRO RJ BR

Cep: Telefone:

Nac: BRASILEIRA

Dt. Nasc.: / /

Cpf: 442.690.647-49

01
A

08

Relatório Descritivo da Patente de Invenção:

"EQUIPAMENTO CHANCELADOR DIGITAL PARA A ASSINATURA DE DOCUMENTOS ELETRÔNICOS, INTERFACE DE PROGRAMAÇÃO DE APLICAÇÃO SEGURA PARA ACESSO A UM EQUIPAMENTO CHANCELADOR DIGITAL, MÉTODOS ELETRÔNICOS PARA CADASTRAMENTO DE IMPRESSÃO DIGITAL UTILIZANDO UM EQUIPAMENTO CHANCELADOR DIGITAL E PARA ASSINAR DIGITALMENTE DOCUMENTOS A PARTIR DA IDENTIFICAÇÃO POSITIVA DE UM USUÁRIO".

ANTECEDENTES DA INVENÇÃO

10 Campo da Invenção

O mundo digital está emergindo com uma velocidade sem precedentes na história humana; governos, empresas e cidadãos desta nova sociedade necessitam de um meio para garantir a privacidade e a autenticidade das transações eletrônicas realizadas à distância. O equipamento digital chancelador (aqui, doravante, por simplicidade, designado simplesmente como chancelador) é um novo tipo de equipamento que utiliza técnicas de biometria, especificamente da impressão digital, para identificar positivamente uma pessoa e, de maneira digital, criptografar, descriptografar, assinar, autorizar e verificar a autenticidade de transações e documentos eletrônicos, utilizando as técnicas de criptografia de chave pública, assinatura e certificação digital.

25 Em vista disso, a presente invenção refere-se à criptografia, assinatura e certificação digitais; mais particularmente, esta invenção desenvolve métodos e equipamentos novos e aperfeiçoados para criptografar, descriptografar, verificar e assinar documentos, de maneira digital, em um dispositivo computacional, a partir da identificação positiva de indivíduos, através do uso de técnicas de biometria, especificamente, de impressões digitais, associadas ao uso de cartões inteligentes.

Descrição da Técnica Relacionada

Atualmente, existem diversos sistemas para proteger e autenticar digitalmente (de maneira digital, empregando técnicas de computação e criptografia) um documento, procurando validá-lo legalmente dentro do mundo eletrônico, especialmente nas transações comerciais ligadas às facilidades implementadas pelo uso da Internet.

Nestes sistemas, um usuário, que deseja obter um certificado digital (CD) emitido por uma autoridade certificadora (AC), deve se apresentar a uma autoridade registradora (AR), munido de documentos que comprovem a sua identidade no mundo real (CPF, carteira de identidade, etc). Desta forma, a AR, comprovando a legitimidade das provas apresentadas pelo usuário, emite uma Solicitação de emissão de Certificado Digital (SCD) para uma AC, firmando a SCD com sua respectiva assinatura digital (AD). A partir daí, a AC, confiando nas informações atestadas pela AR, emite um CD para aquele usuário.

Um certificado digital (CD) nada mais é do que um conjunto de dados de computador, gerados em observância à Recomendação Internacional ITU-T X.509, que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre um par de chaves criptográficas assimétricas e o seu titular, em conformidade com uma Autoridade Certificadora.

A criptografia é o conjunto de princípios, meios e métodos para a transformação das mensagens (dados) em dados ininteligíveis e vice-versa, protegendo o seu conteúdo contra acessos não autorizados. Somente os conhecedores das chaves de criptografia empregadas para criptografar as mensagens são capazes de as "ler", utilizando essas chaves para retornar os dados ininteligíveis (criptografados) ao seu estado original.

10

A criptografia pode ser de chave simétrica (também chamada de chave secreta), onde uma única chave é utilizada tanto para criptografar (tornar ininteligível) como para descriptografar (tornar novamente inteligível) a
5 informação.

Na criptografia de chaves assimétricas (também chamada de chave pública), empregamos um par de chaves criptográficas que são assimétricas quanto a sua funcionalidade (toda informação criptografada com uma das
10 chaves somente poderá ser descriptografada com a outra). Uma das chaves desse par (a chave pública) deve ficar disponível para qualquer pessoa que queira criptografar informações que somente possam ser "lidas" pelo usuário titular desse par de chaves; portanto, essa chave é de
15 domínio público. A chave privativa deve ser mantida em total sigilo pelo seu usuário titular: ela é o principal segredo deste "cofre"; ela permite ao seu usuário titular descriptografar mensagens endereçadas a ele e assinar suas mensagens digitalmente.

20 A chave pública de criptografia consta do próprio CD. A chave privativa deverá ficar sob a guarda exclusiva do titular do CD em algum meio magnético confiável.

O usuário titular deve ter o máximo cuidado com a sua chave privativa, pois qualquer um, que tenha acesso a
25 ela, poderá assinar digitalmente qualquer documento eletrônico em seu nome, além de poder descriptografar documentos endereçados a ele.

A chave privativa e o certificado digital são instalados no computador do usuário, usualmente armazenados
30 localmente no disco rígido ou em um disquete.

A partir daí, quando o usuário necessitar enviar um documento pela rede, garantindo a sua originalidade (as suas integridade e procedência), ele submete este documento

a um processo computadorizado de assinatura digital.

A assinatura digital é um processo criado pela geração de um registro sumário do documento original (por utilização de uma função hash que se baseia em técnicas de criptografia irreversível). Esse registro sumário do documento original é criptografado, utilizando a chave privativa do autor ou remetente desse documento, dando origem à assinatura digital do documento. Esta assinatura digital comprova a originalidade do documento, uma vez que vincula o seu conteúdo original (utilizado para se obter o registro sumário) e a chave privativa de criptografia do seu autor ou remetente (utilizada para criptografar o registro sumário obtido no passo anterior). Isso é semelhante ao mundo real, quando assinamos um documento, de próprio punho, para cancelarmos o mesmo por escrito.

Uma função hash, baseada em algoritmo de criptografia irreversível, aplicada a um documento ou mensagem, é capaz de resumir todo o seu conteúdo a um número único (resumo do documento ou da mensagem) de maneira que, sempre que aplicada àquele documento ou mensagem obter-se-á o mesmo número (ou resumo). Essa função tem duas propriedades fundamentais: não é possível retornar-se ao documento ou mensagem originais a partir do seu resumo (número); e ela é única, não havendo outros documentos ou mensagens que resultem nesse mesmo número (ou resumo). Ocorrendo uma modificação mínima no documento ou mensagem, a aplicação da função hash, nesse documento ou mensagem, gerará um número ou resumo distinto do gerado na sua aplicação ao documento ou mensagem original.

Os sistemas atuais apresentam alguns pontos vulneráveis, que podem comprometer a segurança e a confiabilidade desse processo.

O primeiro deles é o próprio método de

12

identificação do usuário. Por maior que seja a sua probidade e por maiores que sejam os cuidados que uma autoridade registradora possa ter, nunca se poderá garantir que os documentos e provas apresentados sobre a identidade
5 do usuário possam ser isentos de fraude, isto é, que aquela pessoa que se está apresentando fisicamente seja, de fato, a que consta nos documentos.

Além disso, a chave privativa fica armazenada em um ambiente de processamento pouco seguro (normalmente no
10 computador pessoal do usuário), o qual pode ser acessado e violado com muita facilidade.

Finalmente, o processo de assinatura digital também é efetuado num ambiente de processamento pouco seguro e violável, com pouca proteção contra acesso não
15 autorizado à chave privativa. Isto permite que um indivíduo, que não o usuário titular, mal intencionado ou não, possa emitir um documento eletrônico naquele computador ou, até mesmo, fraudar, adulterar, forjar ou corromper um documento assinado pelo legítimo titular
20 daquela chave privativa e correspondente certificado digital.

Procurando diminuir estas vulnerabilidades, soluções foram disponibilizadas no mercado, atenuando suas consequências, ou, até mesmo, solucionando algumas destas
25 situações de forma isolada.

Uma forma simples de se proteger o processo de assinatura digital é o mecanismo de senha de acesso. Esta solução é amplamente difundida, mas, também apresenta problemas de segurança, tais como: a sua divulgação
30 intencional ou não (essa senha pode ser copiada, revelada ou descoberta maliciosamente), através de tentativas sistemáticas ou pela sua captura por mecanismos de interceptação do teclado do computador.

Buscando eliminar essas deficiências, surgiram algumas soluções de identificação por métodos biométricos, uma vez que estes mecanismos utilizam características físicas do indivíduo para assegurar legitimamente a sua
5 identificação. Desta forma, a identificação é feita não mais por informações que as pessoas conheçam (como uma senha, conforme descrito acima), mas, por algo que elas sejam portadoras exclusivas. Um exemplo disso são as impressões digitais, que é sabidamente um atributo único de
10 um ser humano e realmente intransferível. Este método de acesso, além de identificar, autentica a pessoa, pois somente ela possui aquela impressão digital específica.

Esse mecanismo de acesso praticamente resolve o problema de identificação e de autenticação no acesso e na
15 produção de uma assinatura digital.

Contudo, um dos aspectos mais importantes ainda carece de uma solução definitiva: a inviolabilidade do ambiente de processamento da assinatura digital. Soluções foram apresentadas, nas quais o processo de assinatura
20 digital é executado em um dispositivo externo, supostamente seguro, que processa a assinatura digital extraíndo a chave privativa residente no computador do usuário (ambiente vulnerável).

A solução mais difundida para a questão da
25 inviolabilidade, é o uso de cartões inteligentes (smartcards), como geradores e armazenadores da chave privativa e do certificado digital do usuário.

SUMÁRIO DA INVENÇÃO

A presente invenção fornece técnicas novas e
30 aperfeiçoadas para assinatura digital com procedimentos definidos dentro de um dispositivo computacional autônomo.

BREVE DESCRIÇÃO DOS DESENHOS

Através de diagramas básicos, são especificados

14

os processos mais importantes das diferentes concretizações do cancelador digital, e detalha-se a estrutura lógica do equipamento e os métodos fundamentais para o processo da assinatura digital. Portanto:

5 A Figura 1 descreve os componentes do cancelador digital;

 A Figura 2 descreve e detalha os módulos de hardware que constituem o cancelador digital;

 A Figura 3 descreve e detalha os módulos de
10 software que constituem o cancelador digital;

 A Figura 4 descreve e detalha os módulos de software que constituem o hospedeiro do cancelador digital;

 A Figura 5 é um fluxograma descrevendo uma
15 interface de programação segura da presente invenção;

 A Figura 6 é um fluxograma descrevendo os aspectos estruturais e funcionais do cartão inteligente utilizado na presente invenção;

 A Figura 7 descreve o método de cadastramento de
20 uma impressão digital de acordo com a presente invenção;

 A Figura 8 descreve o método de assinatura digital por meio do uso de uma impressão digital de acordo com a presente invenção.

DESCRIÇÃO DETALHADA DAS CONCRETIZAÇÕES PREFERIDAS

25 Descrição do Cancelador para a Assinatura de Documentos Eletrônicos

 A Figura 1 mostra um diagrama da concretização de um equipamento digital, bloco 1.2, denominado cancelador digital, que tem como objetivo emitir assinaturas digitais
30 de forma segura. O equipamento está conectado a um sistema hospedeiro (por exemplo, um computador PC), bloco 1.1, através de uma interface de comunicação de alta velocidade.

 A Figura 1 mostra, no bloco 1.2, os módulos de

interface que compõem o chancelador digital, a saber:

- Porta para comunicação com o sistema hospedeiro
- Porta para comunicação com dispositivos periféricos auxiliares conectados diretamente no chancelador
- Leitora de cartão inteligente
- Leitora de impressão digital
- Visor Digital
- Teclado multifuncional

Os módulos de interface estão encapsulados em um gabinete de plástico injetado, com dispositivo que impede o acesso físico ao interior do chancelador digital e que as suas operações de entrada e saída sejam interceptadas isoladamente. Dessa forma, os estágios subseqüentes do processo de assinatura digital (obtenção da impressão digital, abertura do cartão inteligente, leitura da chave privativa e do certificado digital, geração da assinatura e transferência do documento assinado para o microcomputador hospedeiro) tornam-se protegidos.

A Figura 2 mostra os módulos de hardware que constituem o chancelador digital, a saber:

- Módulo de visualização
- Módulo de processamento
- Módulo de memória
- Módulo de comunicação
- Módulo de assinatura digital

O módulo de visualização, bloco 2.1, contém a interface para um visor digital, que tem como função exibir as mensagens para o usuário, enviadas pelo hospedeiro ou emitidas pelo chancelador.

O módulo de processamento, bloco 2.2, apresenta um processador baseado em microprocessador, responsável

162

pelas funções de controle, de geração de assinatura digital e de criptografia.

O módulo de memória contém uma memória não volátil, bloco 2.3, para armazenagem do software, das
5 chaves criptográficas, dos certificados digitais e da configuração do cancelador digital e uma memória RAM, bloco 2.4; para a execução do software embarcado e memória temporária do cancelador digital.

Adicionalmente, o módulo de memória contém um
10 dispositivo de proteção antiviolação, bloco 2.5, que impede o acesso indevido às informações sigilosas armazenadas no equipamento.

O módulo de comunicação é composto por uma interface de comunicação com o sistema hospedeiro, bloco
15 2.6, e por uma interface para conexão de dispositivos periféricos auxiliares diretamente no cancelador (impressora, etc.), bloco 2.7.

O módulo de assinatura digital é formado por uma interface com o cartão inteligente, por uma interface de
20 impressão digital e por um gerador de ruídos.

A interface do cartão inteligente, bloco 2.8, é responsável pela implementação dos protocolos de comunicação entre o cancelador e o cartão inteligente e funções de controle do leitor do cartão inteligente.

25 A interface de processamento da impressão digital, bloco 2.9, é responsável pela leitura e processamento da impressão digital.

O gerador de ruído, bloco 2.10, tem como propósito fornecer números aleatórios de alta qualidade,
30 para os algoritmos de criptografia.

A Figura 3 descreve e detalha os módulos de software que constituem o cancelador digital, a saber:

- Módulo de Inicialização
 - Módulo Gerenciador de Comunicação
 - Módulo Assinatura Digital
 - Kernel (Núcleo do Sistema Operacional) e Drivers
- 5 (Controladoras dos Dispositivos)

O módulo de inicialização é composto das rotinas de carga do sistema, bloco 3.1, de teste dos dispositivos de hardware, bloco 3.2, de teste de memória, bloco 3.3, e de testes dos certificados digitais e chaves de criptografia, bloco 3.4.

10

O módulo gerenciador de comunicação é composto dos seguintes elementos: gateway com o cartão inteligente, no processador de comandos e no processador do protocolo de comunicação hospedeiro-chancelador.

15 A gateway com o cartão inteligente, bloco 3.5, é a responsável pelo tratamento das mensagens da aplicação que fluem diretamente entre o hospedeiro e o cartão inteligente. Essas mensagens estão formatadas segundo o padrão ISO 7816 nível 3 (APDU). A gateway decide quais

20 mensagens devem ser encaminhadas transparentemente para o cartão inteligente e quais deverão receber tratamento parcial ou total do chancelador.

O processador de comandos, bloco 3.6, executa os comandos do chancelador enviados pelo hospedeiro ou as APDUs que a gateway com o cartão inteligente tenha submetido para serem tratadas diretamente.

25

O processador do protocolo hospedeiro-chancelador, bloco 3.7, é responsável pela integridade e pelo sigilo da comunicação entre hospedeiro-chancelador.

30 O módulo de assinatura digital é composto pelo gerenciador de certificados, gerenciador de chaves e das funções de criptografia, hash, assinador de mensagens,

inicialização do cartão inteligente e API (sigla, em inglês, para Interface de Programa de Aplicação) de acesso ao cartão.

A função do gerenciador de certificados, bloco 3.8, é gerar, instalar, renovar, revogar e remover certificados digitais no cancelador.

O gerenciador de chaves, bloco 3.9, é responsável pela geração de chaves assimétricas, para os algoritmos de criptografia de chave pública implementados no cancelador, e simétricas (ou de sessão), para os algoritmos de criptografia de chave secreta implementados no cancelador.

A função de criptografia, bloco 3.10, implementa os algoritmos assimétricos (RSA, ECC, entre outros) e os algoritmos simétricos (3DES, RC2, AES, entre outros) utilizados interna e externamente ao cancelador.

A função de hash, bloco 3.11, implementa os algoritmos de criptografia irreversível (SHA-1, MD5, entre outros), utilizados para geração e verificação de assinaturas digitais e verificação da integridade do próprio cancelador.

A função do assinador de mensagens, bloco 3.12, é assinar digitalmente a mensagem enviada pelo hospedeiro, com a chave privativa do usuário armazenada no cartão inteligente e devolvê-la armazenada em envelope digital de segurança assinado digitalmente pelo próprio cancelador.

A função de inicialização do cartão inteligente, bloco 3.13, fornece todos os recursos necessários à criação e armazenamento, no cartão inteligente, das chaves de criptografia, certificados digitais e informações biométricas para identificação positiva dos seus titulares. O processo consiste em: montar todos os componentes necessários a um CD dentro do padrão PKCS#10 (SCD), gerar a chave pública e a chave privativa do usuário titular do

119

cartão, capturar as suas impressões digitais e codificá-las (templates) e gravar este pacote de informações nas áreas privadas do cartão inteligente. A função, então, envia ao hospedeiro o pacote SCD para ser validado por uma AC e, ao
5 receber o CD da AC (SCD validado pela AC), o instala no cartão inteligente, habilitando o seu uso.

A API de acesso ao cartão inteligente, bloco 3.14, tem como objetivo implementar as funções de autenticação, de leitura e de gravação do cartão
10 inteligente.

O módulo Kernel & Drivers tem como função o controle do hardware do cancelador e é composto pelos seguintes drivers de dispositivos: comunicação com o hospedeiro, bloco 3.15; comunicação com dispositivos
15 periféricos auxiliares, bloco 3.16; controle da interface com o cartão inteligente, bloco 3.17; controle da interface com o leitor de impressão digital, bloco 3.18; e controle do visor digital, bloco 3.19.

A Figura 4 descreve e detalha os módulos de software que constituem o hospedeiro do cancelador digital, a saber:
20

- Módulo de funções de inicialização do cancelador
- Módulo de funções administrativas do cancelador
- Módulo de funções para assinatura e criptografia
- 25 • Kernel e Drivers

O módulo de funções para inicialização do cancelador tem como função colocar o cancelador em estado operacional. Ele é composto pelas rotinas de inicialização de fábrica, bloco 4.1, e de inicialização de campo, bloco
30 4.2.

A rotina de inicialização de fábrica, bloco 4.1, tem como objetivo instalar software, serializar ("gravar" o

número de série do equipamento no próprio), gerar chaves criptográficas, gerar SCDs, instalar CDs das AC e do fabricante no cancelador.

5 A rotina de inicialização de campo, bloco 4.2, instala, renova, na mesma autoridade certificadora, recertifica, em outra autoridade certificadora, o CD do cancelador, e ativa o cancelador (o coloca em estado operacional). A ativação do cancelador consiste da geração, no campo, da SCD do cancelador, da sua
10 transmissão ao fabricante, da sua transformação em CD, e da instalação desse CD no cancelador, que só então se torna apto a funcionar.

O módulo de funções administrativas do cancelador é composto pelas rotinas de inicialização do
15 equipamento ("liga" o cancelador, sincronizando-o com o hospedeiro), bloco 4.3; de recuperação de log (retorna o último envelope digital de segurança transmitido para o hospedeiro), bloco 4.4; de recuperação da identificação da última transação feita pelo cancelador (retorna o último
20 NSU - número seqüencial único que identifica cada envelope digital de segurança criado pelo cancelador), bloco 4.5; de solicitação de CDs armazenados no cancelador (pode ser o do próprio cancelador, o do fabricante ou o de uma das CA conhecidas pelo cancelador), bloco 4.6; de solicitação
25 do CD do usuário (armazenado no cartão inteligente), bloco 4.7; de solicitação do hash do software do cancelador (para verificação da integridade do software do cancelador), bloco 4.8; de solicitação do CRC de faixas da memória do cancelador (do inglês Circular Redundancy
30 Check) para verificação da sua integridade, bloco 4.9; e de atualização do cancelador (software básico, software aplicativo, parâmetros internos, diálogos e mensagens para o usuário, instalação de CDs e outros), bloco 4.10. A

atualização do cancelador se dá pelo recebimento de uma ou mais mensagens contendo arquivos de dados criptografados com a chave pública do cancelador e assinados digitalmente, pelo fabricante do cancelador. O cancelador, ao receber essas mensagens, verifica a sua integridade (confere se a assinatura digital do fabricante confere) e, caso confira, as descriptografa. (com a sua chave privativa) e usa o seu conteúdo para atualizar a si próprio. As demais funções desse bloco não requerem serem assinadas digitalmente. Todas as respostas dos comandos administrativos dados ao cancelador se fazem através do envio, ao hospedeiro, de mensagens contidas em envelopes digitais de segurança assinados digitalmente pelo próprio cancelador garantindo, assim, a sua originalidade (integridade e procedência).

O módulo de funções da API do cancelador consiste nas rotinas de assinatura com a chave privativa do usuário (armazenada no cartão inteligente), bloco 4.11; de verificação da integridade de um envelope digital de segurança, bloco 4.12; de criptografia de mensagem com a chave pública do destinatário, bloco 4.13; e de descriptografia da mensagem destinada ao usuário titular do cartão inteligente, bloco 4.14. Em resposta às rotinas desse módulo o cancelador enviará, ao hospedeiro, mensagens armazenadas em envelopes digitais de segurança assinados digitalmente pelo próprio cancelador garantindo, assim, a sua originalidade (integridade e procedência). As mensagens conterão a mensagem processada, em caso de sucesso, ou uma mensagem de erro, caso ocorra algum problema com o seu processamento.

O módulo Kernel & Drivers tem como função controlar a comunicação entre o hospedeiro e o cancelador e entre esse e o mundo externo. Ele é constituído pelo

driver de comunicação hospedeiro-chancelador, bloco 4.15, do driver de comunicação (gateway) cancelador-mundo externo, bloco 4.16 e da interface para acesso direto ao cartão inteligente, bloco 4.17.

5 Uma interface de programação de aplicação segura para
 acesso ao cancelador (APIseg)

A figura 5 mostra um fluxograma descrevendo uma interface de programação segura da presente invenção. A interface de programação de aplicação segura (APIseg) é
10 formado por um conjunto de funções disponíveis para um programa de aplicação, bloco 5.1, que necessita fazer operações de administração do cancelador de forma segura.

O módulo de administração, bloco 5.2, implementa as transações que são disparadas pelo microcomputador para
15 manutenção do cancelador.

A aplicação, antes de submeter uma operação via a APIseg, deverá executar uma rotina, que compreende os seguintes passos: criação do bloco de controle, bloco 5.1.1; preenchimento do bloco de controle com os dados
20 apropriados, bloco 5.1.2; assinatura digital do bloco de controle, bloco 5.1.3; e submissão do bloco de controle a APIseg, bloco 5.1.4.

O módulo de administração executa uma rotina, que compreende os seguintes passos: recebimento do bloco de controle, bloco 5.2.1; descriptografa o bloco, bloco 5.2.2, testa para verificar se o bloco de controle está corretamente assinado, com a chave privativa do proprietário, bloco 5.2.3; execução da operação solicitada, caso o resultado do teste seja positivo, blocos 5.2.4; ou
25 rejeição da operação, caso o resultado do teste seja negativo, blocos 5.2.5.

A API segura é a primeira barreira que garante a inviolabilidade das operações de assinatura digital do

próprio chancelador, porque apenas as aplicações feitas pelo usuário do chancelador e devidamente certificada por este único usuário poderão ter acesso às facilidades implementadas. Dessa forma, qualquer tentativa de ataque com o uso da violência ficará inviabilizada por este processo de certificação local.

Método eletrônico para a abertura da área privada de um cartão inteligente

A Figura 6 exibe um fluxograma descrevendo os aspectos estruturais e funcionais do cartão inteligente utilizado na presente invenção. Mais especificamente, trata-se de um método eletrônico para a abertura da área privada de um cartão inteligente a partir de um template de impressão digital, composto por:

- um cartão inteligente, bloco 6.1;
- um arquivo contendo o número de identificação pessoal (PIN) do proprietário do cartão, bloco 6.1.1;
- um arquivo contendo a chave de sessão do chancelador, bloco 6.1.2;
- um ou mais arquivos contendo as informações relativas às impressões digitais do proprietário do cartão, bloco 6.1.3;
- um arquivo contendo a chave pública do proprietário do cartão bloco, 6.1.4;
- um arquivo contendo a chave privada do proprietário do cartão bloco 6.1.5;
- rotina de extração do template da impressão digital, bloco 6.2;
- rotina de comparação de templates de impressão digital, bloco 6.3;
- rotina de abertura do cartão inteligente, bloco

24

6.4.

O processo de abertura do cartão começa com a execução da rotina de extração do template, que está criptografado, com a chave de sessão do cancelador, e armazenado, em um arquivo, no cartão inteligente.

A rotina de extração de template executa os seguintes passos: leitura da chave de sessão do cancelador, armazenada no cartão inteligente, bloco 6.2.1; descriptografia da chave de sessão, usando uma chave privativa adequada e o algoritmo RSA, bloco 6.2.2; leitura do arquivo de impressão digital, bloco 6.2.3; descriptografia do arquivo de impressão digital, usando a chave de sessão do cancelador e o algoritmo triple-DES, bloco 6.2.4; extração do template da impressão digital do arquivo de impressão digital já descriptografado, bloco 6.2.5.

Após a conclusão, com sucesso, da rotina de extração de templates, o próximo passo é verificar se o template extraído do cartão é compatível com a impressão digital lida pelo cancelador, por intermédio da rotina de comparação de templates de impressão digital. Os seguintes passos serão realizados: leitura da impressão digital do usuário, bloco 6.3.1; geração de template da impressão lida, bloco 6.3.2; comparação do template da impressão lida com o template extraído do cartão, bloco 6.3.3, teste para verificar se os templates são compatíveis, bloco 6.3.4; retorno de uma resposta negativa ou positiva, conforme o resultado da operação, blocos 6.3.5 ou 6.3.6, respectivamente.

Finalmente, a rotina de abertura do cartão é executada. Os seguintes passos serão realizados: extração do código de PIN do arquivo de impressão digital anteriormente descriptografado, bloco 6.4.1; envio do

25

código de PIN para o cartão, bloco 6.4.2; teste para verificar se o cartão foi aberto, bloco 6.4.3; retorno de resposta negativa se não houve sucesso, bloco 6.4.4; do contrário, retorno de resposta positiva, bloco 6.4.5.

5 O método aqui descrito é concretizado em um ambiente à prova de interceptação, porque o cancelador, sendo um dispositivo autônomo, não está sujeito a ter sua memória ou seus dispositivos periféricos monitorados por uma entidade externa.

10 **Método eletrônico para cadastramento de usuários utilizando impressão digital, cartão inteligente e o certificado digital:**

A Figura 7 descreve o método de cadastramento de uma impressão digital de acordo com a presente invenção.

15 Mais precisamente, trata-se de um método eletrônico para cadastramento de usuários utilizando impressão digital, cartão inteligente e certificado digital, compreendendo:

- um cartão inteligente, bloco 7.1;
- um arquivo contendo o número de identificação pessoal (sigla, em inglês, PIN) do usuário titular do cartão inteligente, bloco 7.1.1;
- um arquivo contendo a chave de sessão criada pelo cancelador, bloco 7.1.2;
- um ou mais arquivos contendo as informações relativas às informações biométricas do usuário titular do cartão inteligente, bloco 7.1.3, no caso da presente invenção as impressões digitais do usuário titular do cartão inteligente;
- um arquivo contendo a chave pública do proprietário do cartão, bloco 7.1.4;
- um arquivo contendo a chave privativa do proprietário do cartão, bloco 7.1.5;

- um arquivo contendo o certificado digital do proprietário do cartão, bloco 7.1.6;
- rotina de preparação para cadastramento, bloco 7.2;
- 5 • rotina de cadastramento, bloco 7.3;
- rotina Montagem do SCD, bloco 7.4;
- rotina Armazena Certificado, bloco 7.5.

O processo de cadastramento do usuário começa com a execução da rotina de preparação para cadastramento. Essa
10 é executada através de um comando emitido pelo sistema hospedeiro.

A rotina de preparação para cadastramento executa os seguintes passos: verifica a existência da área do chancelador no cartão inteligente, bloco 7.2.1, e retorna o
15 resultado (positivo ou negativo) para o hospedeiro, bloco 7.2.2.

Após a conclusão, com sucesso, da rotina de preparação para cadastramento, o hospedeiro emite um comando de cadastramento, que ativa a rotina de
20 cadastramento, bloco 7.3. Essa rotina coleta a impressão digital e gera o template da impressão deste usuário, bloco 7.3.1. O próximo passo é executar o processo de geração da chave privativa do usuário, bloco 7.3.2. Posteriormente, é retornado o resultado da coleta de impressão digital com a
25 imagem da mesma, caso a coleta tenha sido positiva, bloco 7.3.3.

A rotina de montagem do SCD é executada após o hospedeiro emitir um comando de montagem do SCD liberando a preparação do envelope X.509 com as devidas informações do
30 chancelador, bloco 7.4.1. É criada uma nova área do chancelador para receber o SCD validado, bloco 7.4.2, e é enviado o SCD já formatado ao hospedeiro, bloco 7.4.3.

Finalmente, a rotina armazena certificado, ativada pelo hospedeiro, inicializa a área privada no cartão inteligente, bloco 7.5.1, armazena o certificado nesta área privada, bloco 7.5.2, e finaliza a operação, retornando ao hospedeiro uma mensagem de término do processo, bloco 7.5.3.

O método aqui descrito é concretizado em um ambiente à prova de interceptação, porque o cancelador, sendo um dispositivo autônomo, não está sujeito a ter a sua memória ou os seus dispositivos periféricos monitorados por uma entidade externa.

Método eletrônico para assinar digitalmente documentos a partir da identificação positiva de um usuário:

A Figura 8 exibe o diagrama de um método eletrônico para a assinatura digital de documentos a partir da identificação positiva de um usuário. Tal método consiste de um cartão inteligente e um template de impressão digital, que contém os seguintes elementos:

- um cartão inteligente, bloco 8.1;
- um arquivo contendo o número de identificação pessoal (PIN) do proprietário do cartão, bloco 8.1.1;
- um arquivo contendo a chave de sessão do cancelador, bloco 8.1.2;
- um ou mais arquivos contendo as informações relativas às impressões digitais do proprietário do cartão, bloco 8.1.3;
- um arquivo contendo a chave pública do proprietário do cartão bloco, 8.1.4;
- um arquivo contendo a chave privada do proprietário do cartão bloco, 8.1.5;
- um arquivo contendo o certificado digital do

proprietário do cartão, bloco 8.1.6;

- rotina de preparação para assinar, bloco 8.2;
- rotina assina, bloco 8.3.

O processo de assinatura é iniciado com a chamada
5 do método de abertura da área do cartão inteligente.

A rotina de preparação para assinar executa os seguintes passos: uso do método de abertura da área privada do cartão, bloco 8.2.1; teste para verificar o resultado da existência da área privada, bloco 8.2.2; retorno da
10 resposta negativa e interrupção do processo, bloco 8.2.3, ou da resposta positiva para efetuar a assinatura, 8.2.4.

Após a confirmação positiva da existência da área privada no cartão, a rotina assina é iniciada, conforme os passos a seguir: obtenção da chave privativa do usuário no
15 cartão, bloco 8.3.1; obtenção do certificado do usuário no cartão, bloco 8.3.2; execução do hash (MD5 ou SHA1) da mensagem, bloco 8.3.3; criação do envelope padrão X.509, bloco 8.3.4; apresentação do hash apropriado, bloco 8.3.5 e solicitação de confirmação, bloco 8.3.6; a obtenção de
20 resposta negativa interrompe o processo, bloco 8.3.7; resposta positiva concretiza a assinatura digital retornando envelope padrão X.509 assinado, bloco 8.3.8.

O método aqui descrito é concretizado em um ambiente à prova de interceptação, porque o chancelador,
25 sendo um dispositivo autônomo, não está sujeito a ter sua memória ou seus dispositivos periféricos monitorados por uma entidade externa.

REIVINDICAÇÕES

1. Equipamento cancelador digital para a assinatura de documentos eletrônicos, caracterizados pelo fato de compreender:

- 5 leitor de impressão digital;
 leitor de cartão inteligente;
 gerador de assinatura digital;
 interface de comunicação;
 unidade de processamento baseado em
10 microprocessador;
 memória RAM;
 memória não volátil;
 gerador de ruído;
 visor digital;
15 teclado multifuncional.

2. Interface de programação de aplicação segura para acesso a um equipamento cancelador digital, caracterizado pelo fato de compreender:

- uma interface segura para gravação criptografada
20 das chaves do cancelador;
 uma interface segura para validação das assinaturas do cancelador e
 uma área do cancelador contendo as chaves criptografadas.

25 3. Método eletrônico para cadastramento de impressão digital utilizando um equipamento cancelador digital, caracterizado pelo fato de compreender as etapas de:

- captura dos dados do usuário;
30 geração da chave pública e privativa no equipamento digital cancelador;
 coleta da impressão digital no equipamento digital cancelador;

geração de template no equipamento digital
chancelador;

geração de uma senha no equipamento digital
chancelador;

- 5 gravação da senha no cartão inteligente;
 gravação do template no cartão inteligente e
 gravação da chave pública e privativa no cartão
 inteligente.

4. Método eletrônico para assinar digitalmente
10 documentos a partir da identificação positiva de um
usuário, caracterizado pelo fato de compreender as etapas
de:

transmissão do documento do microcomputador⁴ para
um chancelador;

- 15 coleta da impressão digital do usuário;
 geração de um template;
 leitura da senha de abertura do cartão
 inteligente;

- leitura do template a partir de um cartão
20 inteligente;

 comparação desses dois templates;
 geração da assinatura digital e
 transmissão do documento assinado para o
microcomputador.

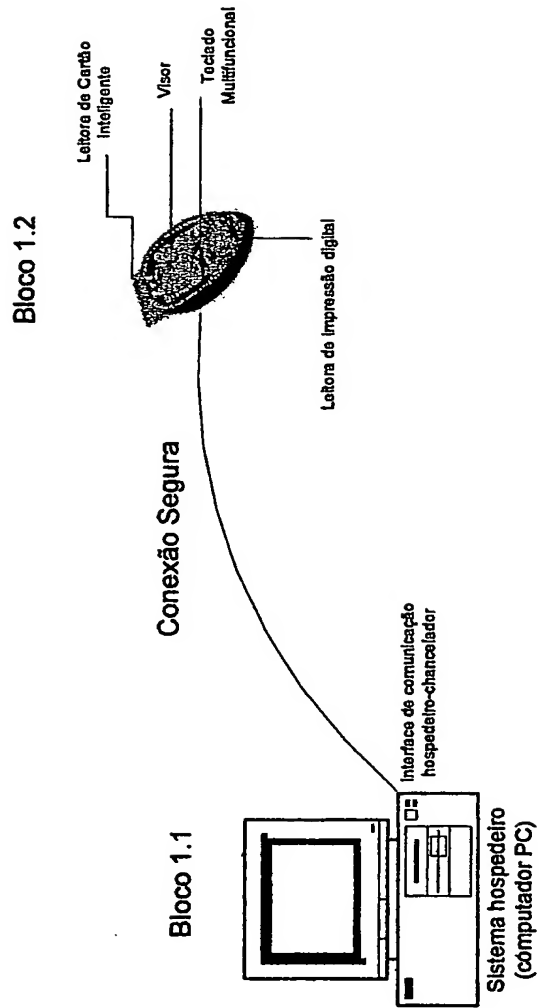


Figura 1

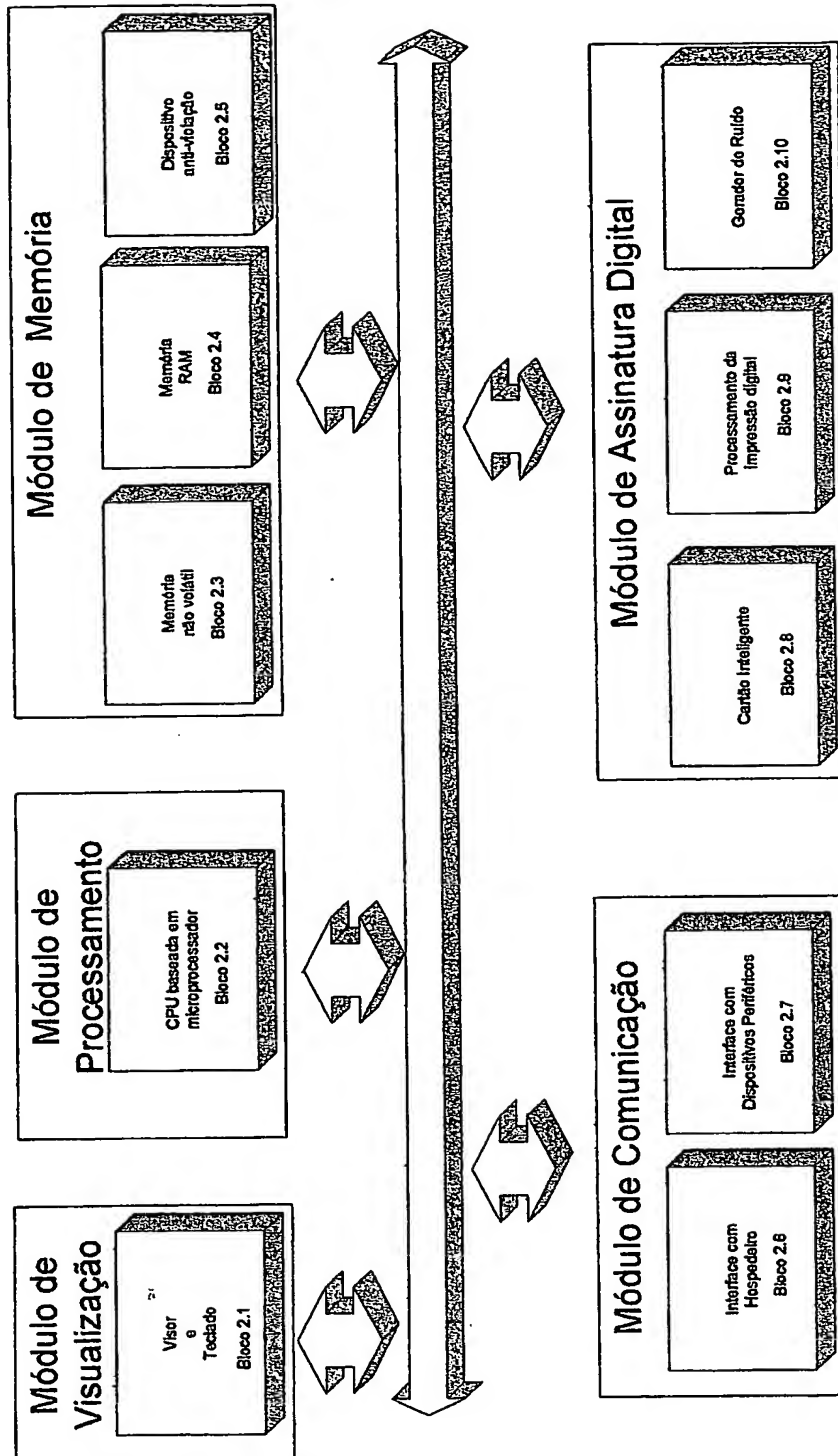


Figura 2

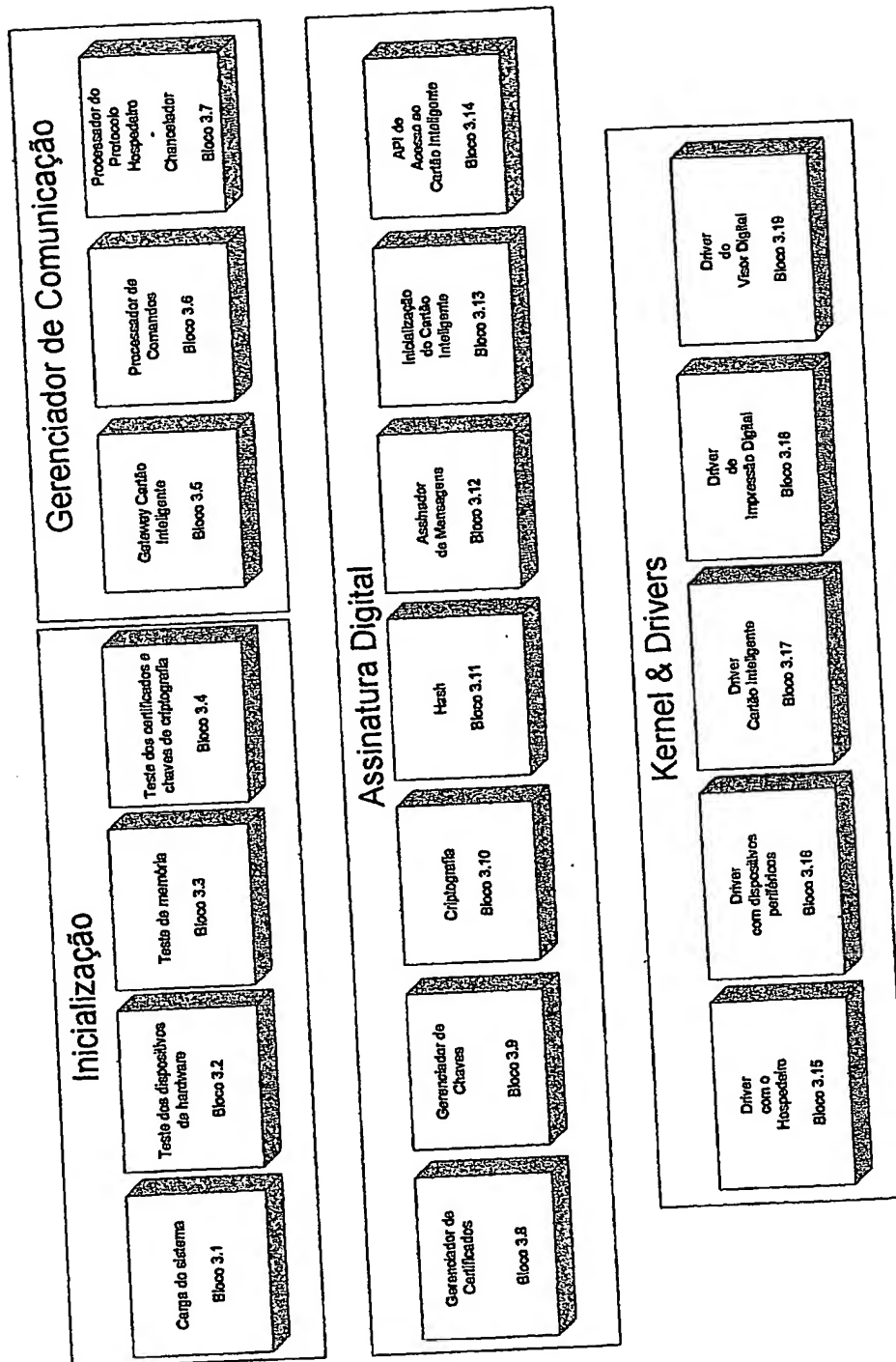


Figura 3

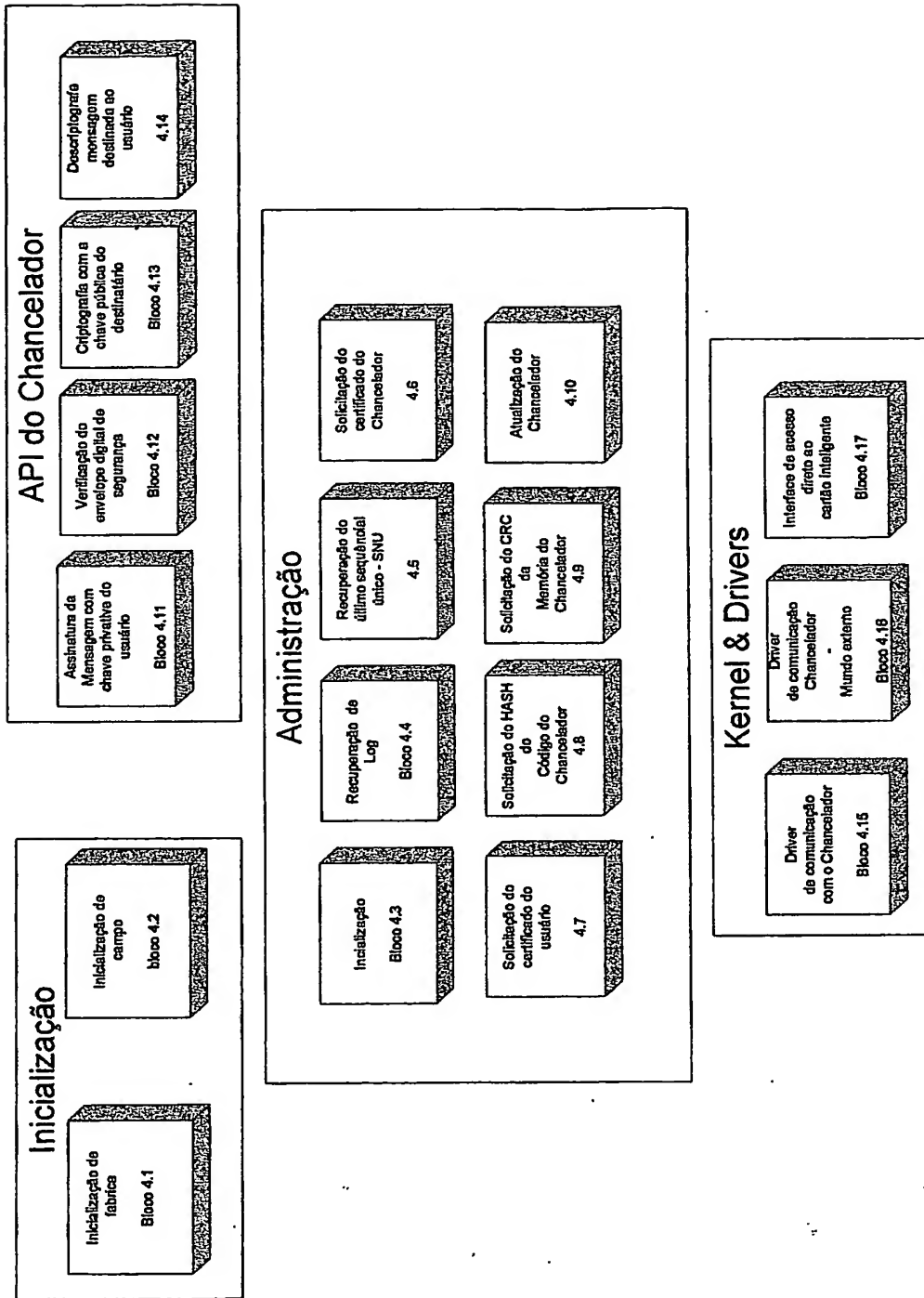


Figura 4

32

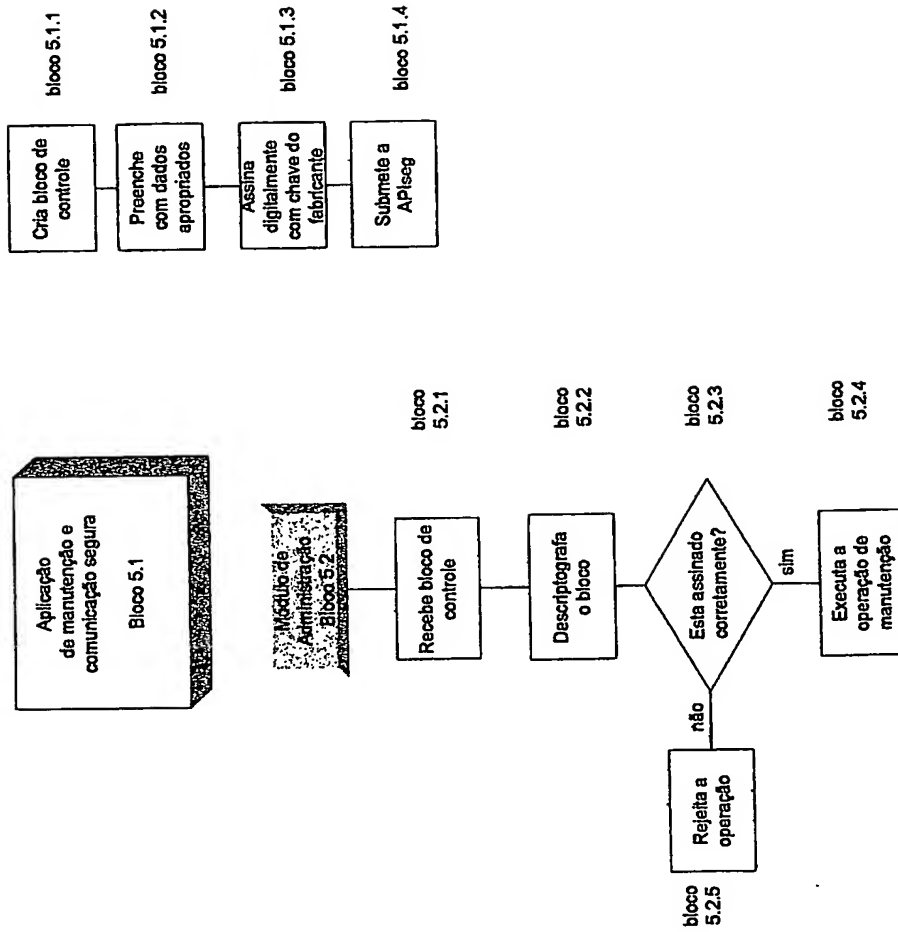


Figura 5

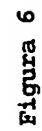


Figura 6

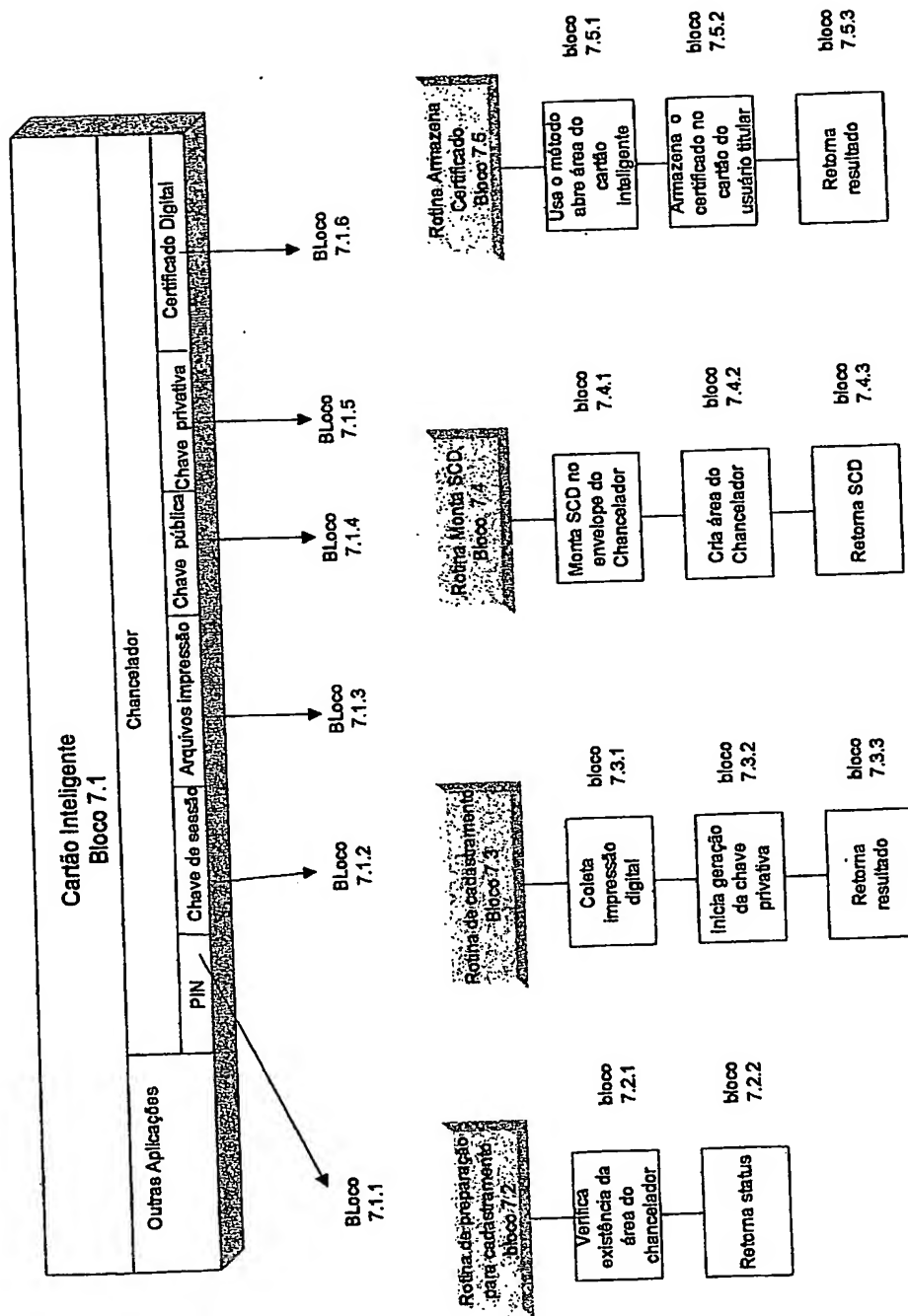


Figura 7

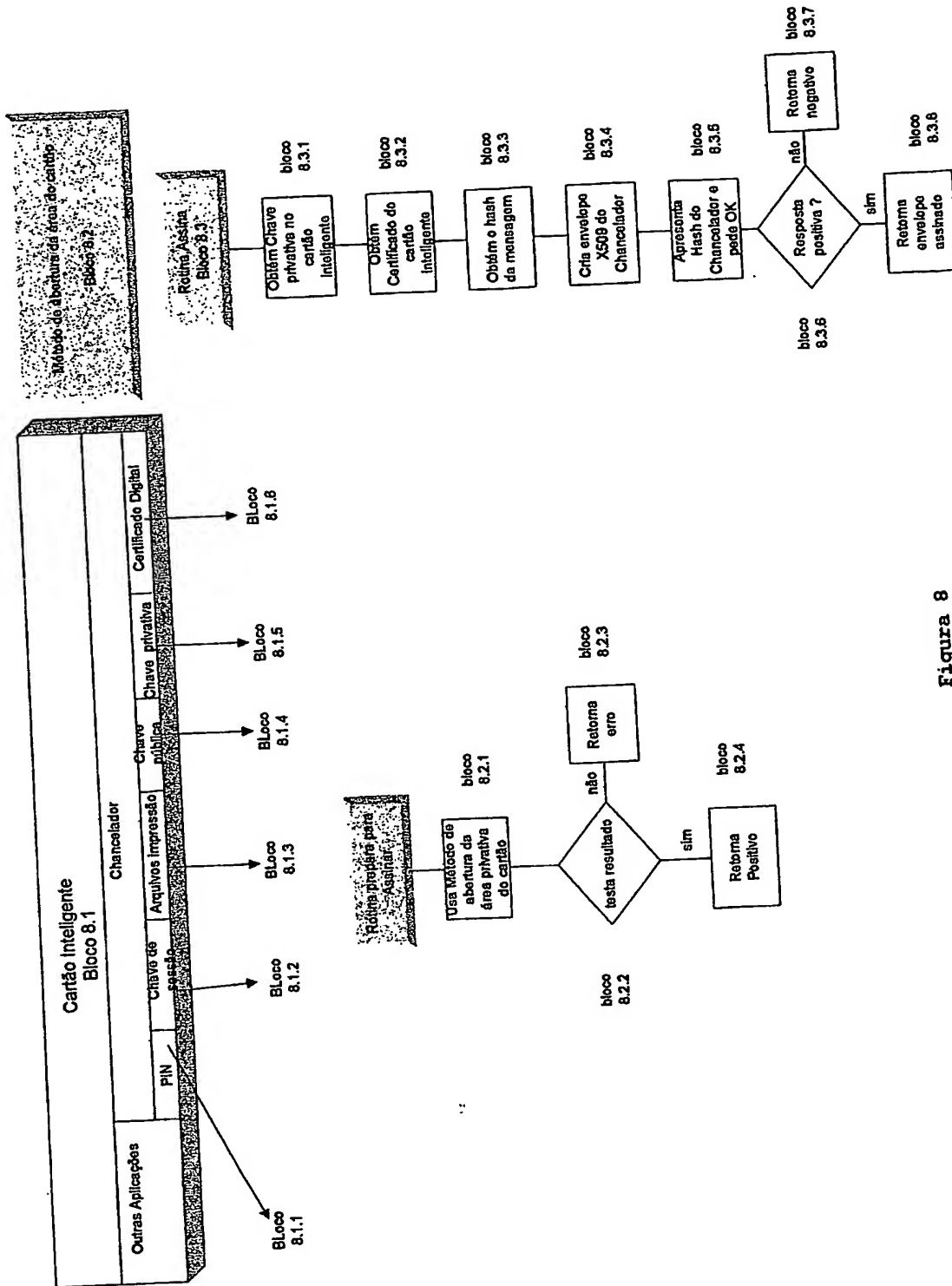


Figura 8

38

RESUMO

Patente de Invenção: "EQUIPAMENTO CHANCELADOR DIGITAL PARA A ASSINATURA DE DOCUMENTOS ELETRÔNICOS, INTERFACE DE PROGRAMAÇÃO DE APLICAÇÃO SEGURA PARA ACESSO A UM EQUIPAMENTO CHANCELADOR DIGITAL, MÉTODOS ELETRÔNICOS PARA CADASTRAMENTO DE IMPRESSÃO DIGITAL UTILIZANDO UM EQUIPAMENTO CHANCELADOR DIGITAL E PARA ASSINAR DIGITALMENTE DOCUMENTOS A PARTIR DA IDENTIFICAÇÃO POSITIVA DE UM USUÁRIO".

A presente invenção refere-se à certificação digital; mais particularmente, esta invenção desenvolve métodos e equipamentos novos e aperfeiçoados para assinar documentos digitalmente em um dispositivo computacional, a partir da identificação positiva de indivíduos, através do uso de técnicas de biometria, especificamente, da impressão digital, e associadas ao uso de cartões inteligentes.